The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
1/12/2010

SUBJECT:
Vulnerability in Microsoft Windows Embedded OpenType Font Engine Could Allow for Remote Code Execution (MS10-001)

OVERVIEW:
A vulnerability has been discovered in the Microsoft Windows Embedded OpenType Font Engine that could allow for remote code execution. Embedded OpenType Fonts are fonts that get embedded in documents such as Microsoft Word, Power Point, or Web pages. This vulnerability can be exploited if a user visits a specially crafted webpage or opens a specially crafted file, including e-mail attachments.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

Windows 2000
Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Embedded OpenType (EOT) Font Engine that could allow remote code execution. This vulnerability occurs in the way the EOT Font Engine

decompresses specially crafted EOT fonts. The vulnerability can be exploited by visiting a specially crafted webpage or opening a specially crafted file, such as an email attachment. In an email scenario the attacker would need the user to open an attachment or click a link to a specially crafted webpage.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patch provided by Microsoft immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-001.mspx

Security Focus:
http://www.securityfocus.com/bid/37671

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0018